ABSTRACT OF THE DISCLOSURE

A methods for preparing an authenticable and verifiable image of a software module by adding to the received software module image a size and location block, an authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key, and a verification block that includes a digital signature prepared from the module image. In one particular embodiment of the present invention, a next firmware-module that is to be accessed during a secure boot process is created to include a module-specific public key, a hashed and encrypted version of the module-specific public key, and a digital signature of the firmware-module image prepared using a module-specific private key.